Survey of Intrusion Detection Techniques in LEACH

Sugandha Gupta and Vandita Grover[#1]

[#] *Department of Computer Science, University of Delhi*

***Abstract*— Security of Wireless sensor network (WSN) turn out to be a very important issue with the rapid development of WSN that is vulnerable to a wide range of attacks due to deployment in the hostile environment and having limited resources. Clustered Networks have been proposed to reduce the power consumption in sensor networks. LEACH is a clustering based protocol that lessens energy dissipation in sensor networks. Intrusion detection system is one of the major and efficient defensive methods against attacks in WSN. This paper surveys the basic IDS mechanisms that are applied in LEACH.**

***Keywords*— Wireless Sensor Networks, Cluster-based routing, LEACH, Intrusion Detection Systems, Watchdog-LEACH, Specification based IDS, Intrusion detection IDS**

I. Introduction

Wireless Sensor Networks (WSN) consists of a large number of tiny nodes with sensing, processing, computing and transmitting abilities; which are deployed over a sensing field. These nodes monitor areas, collect required data and route the information back to the base station (often known as sink). These sensor nodes equipped with inadequate battery resource and due to computing and transmission operations; they deplete at a quicker rate. As the applications of wireless sensor networks are growing day by day but on the other hand it faces the critical problem of energy constraints in terms of limited battery lifetime due to the circumscribed energy resources of the sensor nodes.

For effective and efficient utilization of energy resources of a sensor node and to enhance the lifetime of wireless sensor network, the protocols running on wireless sensor networks must efficiently reduce the node energy consumed in order to achieve a longer network lifetime. Thus, data gathering protocols play an important role in wireless sensor networks keeping in view of severe power constraints of the sensor node.

Routing protocols can be classified in two ways; based on the structure of the network and the protocol operation. As per the structure of the network, routing in WSNs can be divided into flat-based routing, hierarchical-based routing and location-based routing. In flat-based routing, all nodes are treated likewise and allocated same roles. In hierarchical-based routing, two layer routing is used which in turn increases the lifetime of the WSN. Location-based routing, addresses sensor nodes based on their location in the network. Location are learned by GPS or via coordination among the nodes. Furthermore, these protocols can also be classified as multipath-based, query-based, negotiation-based, QoS-based and coherent based routing techniques provisional to the protocol operation.

In a hierarchical architecture, higher sensor nodes can be used to process and send the information while the low energy nodes can be used to attain the sensing in the vicinity of the target. Here, sensor nodes are characteristically grouped into clusters on the basis of specific requirements. Within each cluster, one of the sensor nodes is designated as a cluster head (CH) and with the rest being cluster members (CM). Cluster head gathers the data locally from the cluster members, and transmits the accumulated data to the sink. This transmission can either be direct or can use multi-hoping; i.e. if a sensor node cannot communicate with other nodes through a direct link, then intermediate sensor nodes of the network can be used. This data accumulation in the cluster head reduces the energy consumption in the network thus increasing the network lifetime. The principal challenge encountered by this class of routing is selection of cluster heads and cluster formation.

Cluster-based routing algorithms are becoming an active part of routing technology in WSNs on account of a variability of advantages, such as better scalability, less load, better energy consumption, great performance and more robustness. The main problem of clustering algorithm is that energy consumption is focused on the cluster heads thus it's important to resolve how energy consumption may be distributed.

The illustrative solution is LEACH, which is a confined clustering method based on a probability model. LEACH is a clustering-based protocol that lessens energy dissipation in sensor networks. The purpose of LEACH is to select sensor nodes randomly as cluster heads, so the high energy dissipation in communicating with the base station is spread to all sensor nodes in the sensor network.

This paper reviews the LEACH protocol and its functioning in Section II, security vulnerabilities of LEACH protocol in Section III, Intrusion Detection Systems as a solution to security attacks in Section IV and Various Proposed IDS for LEACH in Section V. And finally Section VI concludes our paper.

II. Leach Protocol [1]

Hienzelman et al. [1] proposed Low-Energy Adaptive clustering algorithm for cluster based routing in Wireless Sensor Networks. In LEACH, nodes in a network are arranged as clusters and one of the nodes is selected as cluster head (CH). The remaining nodes in network are called cluster members.

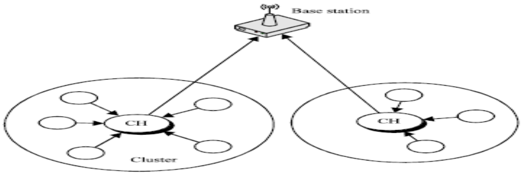


Figure 1 [2]: Clusters in LEACH Protocol

LEACH protocol choses different cluster heads in different rounds and each round comprises of two phases.

A. *Set up Phase*

Advertisement: When a round begins, each node advertises to other nodes in the cluster, the probability with which it can become the cluster head (ADV). This probability is based on current energy level of the node and for how long it has been since it last served as CH. The longer the time it has been CH the higher the chance it has to be elected as CH. ADV is broadcasted using CSMA MAC protocol.

A threshold value T(n) which has been set apriori is used to choose CH. T(n) is determined by

p: desired percentage to become cluster head
r: current round
G: set of nodes that have not become CH in last 1/p rounds

$$T(n) = \frac{p}{1 - p(r modulo(1/p))} if n \in G$$
$$0 otherwise$$

Cluster Setup Phase: CH creates a TDMA schedule based on messages received within the cluster. A random CSMA code is picked. CH then broadcasts the TDMA table to cluster members. A node that wished to become a cluster-head chooses a value, between 0 and 1. If this random number is less than the threshold value, T (n), then the node becomes the cluster- head for the current round.

After being elected as CH, the node advertised to other nodes in network, inviting them to join cluster. Non cluster head nodes become members based on signal strength of advertisement message, by sending the Join-REQ message.

B. *Steady Phase*

Based on TDMA schedule the member node sends data to cluster head. CH aggregates the data received from member nodes. The communication is done using direct-sequence spread spectrum (DSSS) and each cluster uses a unique spreading code to reduce inter-cluster interference. Each cluster head compresses data and sends to Base Station using a fixed spreading code and CSMA.

III. Security Vulnerabilities in LEACH [2]

There are certain design level flaws in LEACH which makes it vulnerable to a number of security attacks aiming towards Denail of Service of the entire network or certain portions of it. The vulnerabilities exist in different layers of the network architecture which makes it susceptible to different DoS attacks.

The LEACH protocol is divided into two major phases: the set-up and steady phases. However, such phases have been divided into four smaller phases to identify easily possible misbehaviors.

A. *Advertisement Phase*

In this phase, each node decides whether it will become the Cluster Header (CH) or not and advertises the decision to other sensor nodes of the cluster. LEACH protocol rely on CHs as all the communication to the Base Station in a network routes through CH only.

Due to this, if a malicious node becomes a CH, the impact of the attack can be severe. There are two possible misbehaviors in this phase of the protocol. First, the malicious node can become a CH uninterruptedly in all rounds, taking benefit of the self CH election characteristic of the LEACH protocol. Second, the malicious node can transmit a strong signal to advertise itself as CH in an attempt to cover a wider cluster range.

B. *Cluster Set up Phase*

In this phase, a sensor node picks the nearest CH and sends a join message to become a member node of its cluster.

The misbehavior that a malicious node can achieve in this phase is to elude the transmission of the join message to join a cluster. This misbehavior results in the omission of transmission of the data sensed by the node.

C. *Schedule Creation*

This phase is executed after the CH receives the join message from the member nodes.

The misbehavior that could happen in this phase is that the CH omits the transmission of the TDMA schedule to the member nodes. With this attack, the member nodes are not able to transmit their sensed data to the base station.

D. *Steady State Phase*

In this phase, the CHs gathers the information transmitted by the cluster member nodes and forward it to the base station.

There are two promising misbehaviors that a member node can execute in this phase. First, the malicious member node can omit the transmission of the sensed data. Second, the malicious node can intentionally transmit data in a time slot that belongs to another node to provoke collision and interfere with normal data transmission.

IV. INTRUSION DETECTION SYSTEMS (IDS)

A Wireless Sensor Network is composed of large number of low cost and resource limited sensor nodes distributed within the sensing field. The sensor nodes do not contain any robust security mechanisms, thus making them susceptible to attacks. Attacks in wireless network can either be an insider attack or an outsider attack. Conventionally security mechanisms like encryption, access control and authentication have been used to address a chunk of the security problems of wireless networks. However, they have not been able to revert aptly to insiders attack in the wireless network environment. Thus, there is a prerequisite of upholding a high level of security in wireless sensor networks.

In order to deliver an approach of safeguarding the vital network functionalities without disturbing their proficiency, intrusion detection was suggested. Intrusion Detection can be defined as a process of monitoring happenings in a system. And, the mechanism by which this is achieved is called an Intrusion Detection System (IDS).

An IDS gathers activity information and then analyses it to conclude whether there are any activities that violate the security aspects of a network’s resource. Once an anomalous activity is identified, it prevents obliteration of the system by sending an alert message to the base station before the intruder starts to attack. Thus, IDS implements three basic functions of monitoring, analysing and reporting to the upcoming attacks in a wireless sensor network. [7]

IDS can be categorized as: [8]

A. Based on Detection Methods

Based on data analysis and detection methods, IDS can be portioned into two categories i.e. Anomaly detection systems and Misuse detection systems.

Anomaly detection systems constructs a model of normal behavior, and compares the model with detected behavior. For this, it firs recognizes normal behaviors and figures out rules for describing a normal behaviour. Then, activities which have surplus deviation from these pre-defined rules are considered as abnormal activities or intrusion efforts. Misuse detection systems are also known as Signature-based detection systems. These systems use deterministic rules and patterns of known attacks to discover security threats and attacks. In these systems, IDS gathers the properties of attacks and abnormal behaviours and then, make a data repository out of it. After pattern and properties matching, IDS can report the type of attack. Also, there exists Hybrid detection systems which is a blend of both anomaly detection systems and misuse detection systems. This amalgam can detect unknown attacks with the high detection rate of anomaly detection and the high accuracy of misuse detection.

B. Based on Architecture

Based on where the IDS is placed in the system and how it seeks information from the system, IDS is categorized as Host-Based Intrusion Detection Systems, Network-Based Intrusion Detection Systems and Distributed IDS.

Host-Based IDS (HIDS) operates on information collected from within an individual computer system, thus formulating precisely which processes and users are involved in a specific attack on the operating system. Network-Based IDS (NIDS) detects attacks by capturing and analysing network packets, i.e. these systems monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts. Distributed IDS (DIDS) is a combination of both HIDS and NIDS.

C. Based on Response Approaches

Once IDSs have obtained event information and analysed it to find symptoms of attacks, they generate responses. Based on how an IDS generates responses, it is classified into Active and Passive response IDS.

Active IDS responses are automated actions taken when certain types of intrusions are detected however Passive IDS responses provide information to system users, trusting on humans to take subsequent actions based on the information.

D. Based on Decision Making

It focuses on who should make the final decision if an intrusion has occurred or not, whether a node is essentially an intruder or not, and what actions should be taken if an attack has truly occurred. IDS is categorized as Cooperative Mechanism IDS and Autonomous Mechanism IDS.

In a cooperative IDS, if a node detects an anomaly, or the current evidences be inconclusive, a cooperative mechanism triggers to produce a global intrusion detection action along with neighbouring nodes; even if a node be sure about the crime of another node, decision making also should be cooperative; because the node which take the judgment, maybe be malicious, itself. In Autonomous IDS, sensor nodes and cluster-heads take decisions, autonomously; they gather proofs and criteria of anomaly and intrusion activities from co-cluster nodes and then, take decision on sensor-level or cluster-level intrusions.

V. VARIOUS PROPOSED IDS FOR LEACH

In this section we discuss a few intrusion detection schemes that have been proposed to add a layer of security in LEACH.

A. WATCHDOG LEACH [4]

Adds security to phases of LEACH to prevent WSN from intruder attack.

Setup Phase: This phase is similar to LEACH set-up but Watchdog nodes are also there to observe possible intrusion (except in the first round). An attack list maintained with Attackid, number of instances of this attack (SUM), Time of attack.

CH sends adv message to all nodes. Watchdog node checks the advertisement message by CH to other nodes for any possible anomaly. If this kind of attack has already taken place, SUM is incremented else the attack is listed with SUM = 0 and Time of attack.

When nodes send join request to CH (given CH is not added to blacklist), the request messages are analysed for possible attack and if found guilty SUM is incremented or new attack is added to the list.

CH then shares TDMA schedule depending on the number of nodes that have joined. Each message with TDMA schedule to other n-1 nodes is analysed for attack and added to list if there is any.

Watchdog Selection Phase:

Spontaneous watchdog approach is adopted to select the watchdog nodes. A node when selected as watchdog activates a monitoring module loaded onto it. Monitoring module analysed packets sent or received by its neighbours in the clusters. A watchdog node receives all communication inside a cluster.

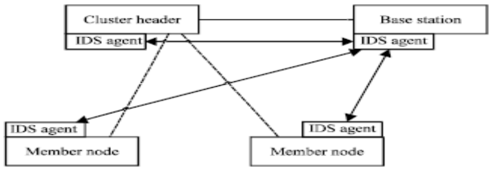
A node may select itself as a watchdog with the probability 1/n (n is number of nodes in the cluster). The node that was CH in previous round will not be considered to be selected as watchdog in current round.

A node with probability 1/n selects itself as watchdog, where $w \notin CH$

Steady and Intrusion Detection Phase:

In this phase all data communication between nodes (other than watchdog) and CH, communication between CH and B.S. is analysed. If there is an intrusion it is added to attack list or SUM is updated. If SUM reaches a pre-defined threshold value that node is blacklisted.

Watchdog nodes monitor both CH and member nodes by listening to communications. A De-centralized Intrusion Detection Approach [ ] is used for detecting attacks and sending alarms to B.S. After end of each round the B.S. communicates the list of black-listed nodes so that all nodes may ignore messages from them and these nodes are not chosen as CH.



Intrusion Detection Algorithm

1. Data Acquisition: Collect messages in promiscuous mode, filter and store in array data structure for future analysis.
2. Rule Application: Apply rules to stored data and increment failure counter if message fails in one of the rules or raise failure if message analysis fails tests being applied.
3. If message failure rate crosses a threshold value, the watchdog node raises an alarm to B.S. Attack is indicated when abnormal behaviour is higher than expected.

RULES

Interval Rule: can detect negligence and exhaustion attack. An alarm is raised if time elapsed between reception of two consecutive messages is larger or smaller.

Retransmission Rule: can detect black hole or selective forwarding attack. Monitor listens messages related to one of its neighbours and expects it to forward the message, but if under influence of intruder, the node will suppress some or all messages.

Integrity Rule: Message integrity must remain intact along the entire path. If intruder manipulates the message this rule will help in detecting it.

Delay Rule: Retransmission of a received message must occur within a stipulated time, else the attack may be detected.

Repetition Rule: can detect the attack that a node transmits same message repeatedly. This rule sets a limit to which a node can retransmit a single message.

Jamming Rule: checks that number of collisions associated with a message must be less than the number expected in a network. If an intruder tries to disrupt communication by introducing noise, jamming rule may help detect the problem.

Radio Transmission Range Rule: If a node is sending more powerful messages as compared to a specified range it may be signal of a hello-flood or wormhole attack.

Alarm Rule: A failure is raised when a sensor is tampered, re-programmed or moved.

Intruder Watchdog Rule: If a watchdog itself is intruder, it may be recognised by this rule. In such a scenario intruder will send invalid information to BS, thereby identifying itself.

B. Specification Based Intrusion Detection Mechanism [2]

Figure 2 [2]: Specification Based IDS in Leach Protocol

The architecture proposed by Lee and Lee [] is based mainly on the distributed and cooperative intrusion detection architecture [ ] proposed by Zhang and Lee (2003) to detect misbehaviors. To enhance lifetime of the sensor nodes, they have used powerful energy and performance capacity feature of the base station. Any misbehavior detected by the nodes (CHs and member nodes), is transmitted to the base station which in turn analyses the data to decide what action to take.

Workload of nodes is reduced as the analysis of data related to misbehavior is delegated to BS, owing to better energy and performance capacity.

Misbehavior detection: There are six identified misbehaviors subject to identification which the proposed IDS can identify.
Continuous header election: Basic assumption is that malicious nodes can't change node's id as it is cryptographically protected. The current CH identification is compared with the elected CH identification. In its memory, every node stores the identification of the elected CH and during new setup phase, the new CH identification is compared with the previous one. Misbehavior is reported if the number of comparisons that are true is greater than a threshold value.

Transmission of a strong signal: It's important to determine that the sender is indeed close to the receiver. Real position of the CH candidate can be verified by ensuring that member nodes calculate the distance to CH candidate using signal strength. The member then sends the join message with same signal strength to reach the destination. If a TDMA schedule is received as response, then only the candidate is noted as CH, else, the node concludes that the candidate has sent a strong signal and identifies this as misbehavior.

No transmission of the TDMA schedule: If the ordinary node transmits the join message to the CH and does not receive a response from it in a predefined period of time, this case is considered as misbehavior.

TDMA schedule disobedience: Node identification in TDMA schedule is compared with the sending node identity. If sender has sent data in slot different than allocated a misbehavior is notified.
No transmission of member Node's data: When a member node does not transmit in the allocated slot CH distinguishes it as misbehavior.

No transmission of head's data: When the CH sends data, the surrounding member nodes can listen to the message. Therefore, if the member nodes do not detect any message from the CH until their next transmission time slot, it is recognized as misbehavior.

C. Intrusion Detection Mechanism Based on Path Information [3]

A secure mechanism to defend WSNs against malicious attacks is proposed by Ying [] using information generated during data communication. This approach is able to protect the data communication in a WSN even if some sensor nodes are compromised. Firstly Ying elaborates how to construct a secure path and then proposes a CUSUM-Based intrusion detection algorithm.

Normal path based data communication: During data communication each normal (behaving normally) sensor node adds its identity to the data packet. On reaching sink, a routing path is constructed which consists of a list of normal sensor nodes i.e. The path is potentially secure and can be used by the source and other nodes. A complete normal path always terminates at the sink and is allocated by the sink. The path is notified to the source node by the sink via the normal path. Notification is sent at intervals to reduce the overall cost of the network. Normal path is a triple <A, L, ΔT> where, where A is the source node for the path, L is the identity list, and ΔT denotes the trust value for a normal path with an initial value λ ($\lambda > 0$). The larger λ, the more secure the path.

Malicious Path Construction
The path from source to sink is expected to be secure if a data packet successfully arrives at sink. Also, it is understood that the path contains at least one malicious node, if a data packet from the source fails to reach the sink. As λ (trust value) decreases to zero or negative the path is removed from cache of sensor nodes and is termed as malicious path and moved to malicious path list.
Malicious paths can be used to perform intrusion detection for WSN. Intuitively, the node(s) that appear in more malicious paths are more likely to be malicious nodes. Therefore, frequency of occurrence of each node in malicious paths is an indicator of it being malicious.

CUSUM-Based Intrusion Detection Mechanism
CUSUM is a novel intrusion detection mechanism with light computation load based on malicious paths. CUSUM can detect sharp but continuous increase. The major procedure of detection is as follows.

Let Xn be the number of malicious paths that a node appears in within a time sample Δn and X be the mean value of X ={X1, X2... Xn}.

Let Z = {Z1, Z2... Zn} where Zn = Zn - δ and δ is peak value of normal behaviors for a specific WSN status so that all elements of Z are negative and so is Z.

When an attack occurs insider attack occurs, Zn will suddenly increase to positive. Let h be the threshold value of attack crossing which a decision function indicates one in case of attack and zero value of decision function shows that WSN is running normally.

VI. CONCLUSIONS

In this paper we studied various techniques to identify intrusion in clusters in LEACH protocol.

Watchdog-LEACH is CH and cluster independent and can be used to identify misbehavior of both member and head node. Detection method is decentralized as monitor modules are spread in the network. This method has 2% energy overhead thus is more practical. In specification-based IDS, identified possible misbehaviors in each phase of LEACH. The IDS proposed algorithm to control these misbehavior. Also, a security mechanism based on normal and abnormal flows in network was proposed.

CUSUM-based IDS makes full use of data communication process of WSN. It demonstrates a simple algorithm which identifies normal paths and malicious paths with limited consumption of energy. The algorithm is not very computation and storage intensive.

REFERENCES

[1] Wendi Rabiner Heinzalman, Anantha Chandrakasan, Hari Balakrishnan, "Energy Efficient Protocol for Wireless Microsensor Networks", IEEE, Hawaii Intenational Conference, 2000

[2] Soojin Lee, Yunho Lee and Sang-Guun Yoo, "A Specification based Intrusion Detection Mechanism for LEACH Protocol", Information Technology Journal 11(1): 40-48, 2012

[3] Bishan Ying, "CUSUM-Based Intrusion Detection Mechanism for Wireless Sensor Networks", Journal of Electrical and Computer Engineering, Volume 2014, Article ID 245938

[4] Mohammad Reza Rohbanian, Mohammad Rafi Khan, Alireza Keshavarz-Haddad and Manije Keshtgary, "Watchdog-LEACH: A new method based on LEACH protocol to Secure Clustered Wireless Sensor Networks".

[5] Nancy Alrajei, George Corser, Huirong Fu and Ye Zhu, "Energy Prediction Based Intrusion Detection in Wireless Sensor Networks", International Journal of Emerging Technology and Advanced Engineering, 2014, vol. 4, Issue 2.

[6] Hossein Jadidoleslamy, "A Hierarchical Intrusion Detection Architecture for Wireless Sensor Networks", International Journal of Network Security & its Applications, vol. 3, No.5, Sep. 2011.

[7] Ms. Rachana Deshmukh, Ms. Rashmi Deshmukh and Prof. Manoj Sharma, "Rule-Based and Cluster-Based Intrusion Detection Technique for Wireless Sensor Network", International Journal of Computer Science and Mobile Computing, 2013, Vol. 2, Issue 6, pg. 200 – 208.

[8] Hossein Jadidoleslamy, "A High-level Architecture for Intrusion Detection on Heterogeneous Wireless Sensor Networks: Hierarchical, Scalable and Dynamic Reconfigurable", Wireless Sensor Network, 2011,3, 241 – 26.

[9] Yassine Maleh and Abdellah Ezzati, "A Review of Security Attacks and Intrusion Detection Schemes in Wireless Sensor Network"

[10] Zhang, Y. and W. Lee, "Intrusion detection techniques for mobile ad hoc networks. " ACM WINET J., 2003: 1-16.